UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/761,112	01/16/2001	Richard S. Slevin	20042-7001	3637

35939   7590   11/01/2006

MICHAEL E. WOODS
PATENT LAW OFFICES OF MICHAEL E. WOODS
112 BARN ROAD
TIBURON, CA 94920-2602

EXAMINER
ZIA, SYED

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 11/01/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

<table>
<tr><td rowspan="2" style="text-align:center">Office Action Summary</td><td>Application No.
09/761,112</td><td>Applicant(s)
SLEVIN, RICHARD S.</td></tr>
<tr><td>Examiner
Syed Zia</td><td>Art Unit
2131</td></tr>
</table>

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on <u>10 October 2006</u>.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>1-49</u> is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) <u>1-49</u> is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.

5)☐ Notice of Informal Patent Application

6)☐ Other: _____.

DETAILED ACTION

This office action is in response to amendment filed on October 10, 2006. Original application

contained Claims 1-2. Applicant previously added new Claims 3-49. Applicant previously

amended Claims 1-3, 6, 9-11, 16-17, 24, and 26-49. Applicant's request for reconsideration of

the finality of the rejection of the last Office action is persuasive and, therefore, the finality of

that action is withdrawn. Presently pending claims are 1-49.

Response to Arguments

Applicant's arguments filed on May 03, 2006 with respect to claims 1-49 have been

considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or
> any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and
> requirements of this title.

Claims 47-48 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-

statutory subject matter .In this case nonfunctional descriptive material is recorded on some

computer-readable medium, in a computer or on an electromagnetic carrier signal, it is not

statutory since no requisite functionality is present to satisfy the practical application

requirement. Merely claiming nonfunctional descriptive material, i.e., abstract ideas, stored in a

computer-readable medium, in a computer, on an electromagnetic carrier signal does

not make it statutory. Also, a signal, a form of energy, does not fall within the definitions of

manufacture. Thus, a signal does not fall within one of the four statutory classes of § 101.

Claim Rejections - 35 USC § 103

1.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in
> section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are
> such that the subject matter as a whole would have been obvious at the time the invention was made to a person
> having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the
> manner in which the invention was made.

2.   Claims 1-49 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cromer et al.

(U. S. Patent 6,237,100) and view of Teitelbaum (U. S. Patent 5,872,834).

3.   Regarding Claim 1 Cromer teach and describe a biometric controlled power gate

controlling a power flow from a power source to an electrically powered device, comprising:

        - a circuit of the device energized by the power flow for enabling a startup procedure of a

processor of the device; a biometric-controlled switch, coupled to said circuit between the power

source and said processor, for enabling said energizing of said circuit responsive to an assertion

of a biometric activation signal; and a biometric reader coupled to said biometric-controlled

switch, comprising: a memory for storing a biometric signature; a biometric sensor, coupled to

said memory, for discerning a biometric profile; and a verifier, coupled to said biometric sensor and to said memory, for asserting said biometric activation signal when said biometric profile matches said biometric signature wherein said electronic device is inoperable from the power source until said assertion of said biometric activation signal (Fig.1-3, col.2 line 34 to col.3 line 25, col.4 line 40 to col.5, line 5, and col.5 line 24 to col.6line 15).

Although the system disclosed by Cromer shows the features of the claimed limitation of controlling within a data processing system for the power supplied to the system .The system of Cromer includes an internal power supply for receiving energy from an external source and supplying the energy to the system. The energy is full system power and is required for the system to be fully operable. The system is initially powered-off such that the energy is not initially supplied to the system. A power-on password is established. The internal power supply supplies the energy to the system only in response to a correct entry of the power-on password, wherein the system is inoperable prior to the correct entry of the power-on password.

However, Cromer does not specifically disclose gating functionality using biometric controlled switch.

In an analogous art, Teitelbaum, on the other hand discloses computing environment that relates to methods and device for receiving biometric input information and for providing biometric data to the a switch for establishing a communication link, such as start and stop of access control, between at least a user and the at least a device user is trying to access, and thus providing features and enabling services in dependence upon received biometric data (col.2 line 42 to line 52, and col.4 line 14 to col.15 line 10).

Therefore, It would have been obvious to one ordinary skilled in the art at the time of

invention to combine the teachings of Cromer and Teitelbaum, because Teitelbaum's device

and functionality combined with Cromer's power security unit (PSU), for controlling power to

the system before the start-up, using biometric input by using directly connection would not

only further enhance the existing security structure in the system of Cromer during startup of a

device and access control but will also provide safeguards against attempt by unauthorized

person to breach security of system during start-up or shut-down (Cromer: col.1 line 65 to col.2

line 5, and Teitelbaum: col.9 line 46 to line 65).

4.   Regarding Claim 2 Cromer teach and describe a method for power gating an electronic

device powered from a power source, comprising:

                - discerning a biometric profile of a prospective user of the electronic device; and

comparing said biometric profile to a stored biometric signature of an authorized user of the

electronic device; and thereafter asserting a biometric activation signal to a biometric-controlled

switch when said prospective user is an authorized user, said biometric-controlled switch

interposed between the power source and a circuit of the electronic device for enabling a startup

procedure of said electronic device such that said biometric-controlled switch interrupts power to

said circuit when said activation signal is not asserted wherein said startup procedure is

inoperable from the power source until said assertion of said biometric activation signal (Fig.1-3,

col.2 line 34 to col.3 line 25, col.4 line 40 to col.5, line 5, and col.5 line 24 to col.6line 15).

        Although the system disclosed by Cromer shows the features of the claimed limitation of

controlling within a data processing system for the power supplied to the system .The system

of Cromer includes an internal power supply for receiving energy from an external source and

supplying the energy to the system. The energy is full system power and is required for the

system to be fully operable. The system is initially powered-off such that the energy is not

initially supplied to the system. A power-on password is established. The internal power

supply supplies the energy to the system only in response to a correct entry of the power-on

password, wherein the system is inoperable prior to the correct entry of the power-on password.

However, Cromer does not specifically disclose gating functionality using biometric

controlled switch.

In an analogous art, Teitelbaum, on the other hand discloses computing environment that

relates to methods and device for receiving biometric input information and for providing

biometric data to the a switch for establishing a communication link, such as start and stop of

access control, between at least a user and the at least a device user is trying to access, and thus

providing features and enabling services in dependence upon received biometric data (col.2 line

42 to line 52, and col.4 line 14 to col.15 line 10).

Therefore, It would have been obvious to one ordinary skilled in the art at the time of

invention to combine the teachings of Cromer and Teitelbaum, because Teitelbaum's device

and functionality combined with Cromer's power security unit (PSU), for controlling power to

the system before the start-up, using biometric input by using directly connection would not

only further enhance the existing security structure in the system of Cromer during startup of a

device and access control but will also provide safeguards against attempt by unauthorized

person to breach security of system during start-up or shut-down (Cromer: col.1 line 65 to col.2

line 5, and Teitelbaum: col.9 line 46 to line 65).

5.   Regarding Claim 3 Cromer teach and describe a biometric power gating system for

controlling power from a power source to a circuit, comprising:

an electronic device including the circuit operable from the power provided from the

power source, a biometric-controlled switch, coupled to said electronic device between the

power source and the circuit, for gating the power from the power source responsive to a

biometric activation signal; and a biometric reader for asserting said biometric activation signal

responsive to a verification of a user biometric signature wherein said electronic device is

inoperable from the power from the power source until said biometric activation signal is

asserted (Fig.1-3, col.2 line 34 to col.3 line 25, col.4 line 40 to col.5, line 5, and col.5 line 24 to

col.6line 15).

Although the system disclosed by Cromer shows the features of the claimed limitation of

controlling within a data processing system for the power supplied to the system .The system

of Cromer includes an internal power supply for receiving energy from an external source and

supplying the energy to the system. The energy is full system power and is required for the

system to be fully operable. The system is initially powered-off such that the energy is not

initially supplied to the system. A power-on password is established. The internal power

supply supplies the energy to the system only in response to a correct entry of the power-on

password, wherein the system is inoperable prior to the correct entry of the power-on password.

However, Cromer does not specifically disclose gating functionality using biometric

controlled switch.

In an analogous art, Teitelbaum, on the other hand discloses computing environment that

relates to methods and device for receiving biometric input information and for providing

biometric data to the a switch for establishing a communication link, such as start and stop of

access control, between at least a user and the at least a device user is trying to access, and thus

providing features and enabling services in dependence upon received biometric data (col.2 line

42 to line 52, and col.4 line 14 to col.15 line 10).

Therefore, It would have been obvious to one ordinary skilled in the art at the time of

invention to combine the teachings of Cromer and Teitelbaum, because Teitelbaum's device

and functionality combined with Cromer's power security unit (PSU), for controlling power to

the system before the start-up, using biometric input by using directly connection would not

only further enhance the existing security structure in the system of Cromer during startup of a

device and access control but will also provide safeguards against attempt by unauthorized

person to breach security of system during start-up or shut-down (Cromer: col.1 line 65 to col.2

line 5, and Teitelbaum: col.9 line 46 to line 65).

6.   Regarding Claim 24 Cromer teach and describe a biometric-mediated power gating

method, comprising.

establishing a biometric profile from a prospective user; comparing said biometric profile

to a biometric signature; asserting a biometric activation signal when said profile and said

signature match; and gating, responsive to said biometric activation signal, power from a power

source to an electronic device using a biometric switch coupled to said biometric activation

signal to enable operation of said electronic device wherein said electronic device is inoperable

from said power source until said assertion of said biometric activation signal and wherein said

biometric access control is disposed between said power source and said electronic device to

control said power thereafter (Fig.1-3, col.2 line 34 to col.3 line 25, col.4 line 40 to col.5, line 5,

and col.5 line 24 to col.6line 15).

Although the system disclosed by Cromer shows the features of the claimed limitation of

controlling within a data processing system for the power supplied to the system .The system

of Cromer includes an internal power supply for receiving energy from an external source and

supplying the energy to the system. The energy is full system power and is required for the

system to be fully operable. The system is initially powered-off such that the energy is not

initially supplied to the system. A power-on password is established. The internal power

supply supplies the energy to the system only in response to a correct entry of the power-on

password, wherein the system is inoperable prior to the correct entry of the power-on password.

However, Cromer does not specifically disclose gating functionality using biometric

controlled switch.

In an analogous art, Teitelbaum, on the other hand discloses computing environment that

relates to methods and device for receiving biometric input information and for providing

biometric data to the a switch for establishing a communication link, such as start and stop of

access control, between at least a user and the at least a device user is trying to access, and thus

providing features and enabling services in dependence upon received biometric data (col.2 line

42 to line 52, and col.4 line 14 to col.15 line 10).

Therefore, It would have been obvious to one ordinary skilled in the art at the time of

invention to combine the teachings of Cromer and Teitelbaum, because Teitelbaum's device

and functionality combined with Cromer's power security unit (PSU), for controlling power to

the system before the start-up, using biometric input by using directly connection would not

only further enhance the existing security structure in the system of Cromer during startup of a

device and access control but will also provide safeguards against attempt by unauthorized

person to breach security of system during start-up or shut-down (Cromer: col.1 line 65 to col.2

line 5, and Teitelbaum: col.9 line 46 to line 65).

7.   Regarding Claim 26 Cromer teach a biometrics-mediated power gating method,

comprising:

        a) asserting a biometric activation signal responsive to a verification of a user biometric

signature; and b) gating, responsive to said biometric activation signal, power from a power

source to an electronic device operable from said power using a biometric-controlled switch

operably disposed between said power source and said electronic device wherein said electronic

device is inoperable from said power source until said assertion of said biometric activation

signal (Fig.1-3, col.2 line 34 to col.3 line 25, col.4 line 40 to col.5, line 5, and col.5 line 24 to

col.6line 15).

        Although the system disclosed by Cromer shows the features of the claimed limitation of

controlling within a data processing system for the power supplied to the system .The system

of Cromer includes an internal power supply for receiving energy from an external source and

supplying the energy to the system. The energy is full system power and is required for the

system to be fully operable. The system is initially powered-off such that the energy is not

initially supplied to the system. A power-on password is established. The internal power

supply supplies the energy to the system only in response to a correct entry of the power-on

password, wherein the system is inoperable prior to the correct entry of the power-on password.

However, Cromer does not specifically disclose gating functionality using biometric

controlled switch.

In an analogous art, Teitelbaum, on the other hand discloses computing environment that

relates to methods and device for receiving biometric input information and for providing

biometric data to the a switch for establishing a communication link, such as start and stop of

access control, between at least a user and the at least a device user is trying to access, and thus

providing features and enabling services in dependence upon received biometric data (col.2 line

42 to line 52, and col.4 line 14 to col.15 line 10).

Therefore, It would have been obvious to one ordinary skilled in the art at the time of

invention to combine the teachings of Cromer and Teitelbaum, because Teitelbaum's device

and functionality combined with Cromer's power security unit (PSU), for controlling power to

the system before the start-up, using biometric input by using directly connection would not

only further enhance the existing security structure in the system of Cromer during startup of a

device and access control but will also provide safeguards against attempt by unauthorized

person to breach security of system during start-up or shut-down (Cromer: col.1 line 65 to col.2

line 5, and Teitelbaum: col.9 line 46 to line 65).

8.   Regarding Claim 47 Cromer teach and describe a computer program product

comprising a computer readable medium carrying program instructions for power gating an

electronic device when executed using a computing system, the executed program instructions

executing a method, the method comprising: a) asserting a biometric activation signal responsive

to a verification of a user biometric signature; and b) gating, responsive to said biometric

activation signal, power from a power source to the electronic device operable from said power

using a biometric-controlled switch operably disposed between said power source and the

electronic device (Fig.1-3, col.2 line 34 to col.3 line 25, col.4 line 40 to col.5, line 5, and col.5

line 24 to col.6line 15).

Although the system disclosed by Cromer shows the features of the claimed limitation of

controlling within a data processing system for the power supplied to the system .The system

of Cromer includes an internal power supply for receiving energy from an external source and

supplying the energy to the system. The energy is full system power and is required for the

system to be fully operable. The system is initially powered-off such that the energy is not

initially supplied to the system. A power-on password is established. The internal power

supply supplies the energy to the system only in response to a correct entry of the power-on

password, wherein the system is inoperable prior to the correct entry of the power-on password.

However, Cromer does not specifically disclose gating functionality using biometric

controlled switch.

In an analogous art, Teitelbaum, on the other hand discloses computing environment that

relates to methods and device for receiving biometric input information and for providing

biometric data to the a switch for establishing a communication link, such as start and stop of

access control, between at least a user and the at least a device user is trying to access, and thus

providing features and enabling services in dependence upon received biometric data (col.2 line 42 to line 52, and col.4 line 14 to col.15 line 10).

Therefore, It would have been obvious to one ordinary skilled in the art at the time of invention to combine the teachings of Cromer and Teitelbaum, because Teitelbaum's device and functionality combined with Cromer's power security unit (PSU), for controlling power to the system before the start-up, using biometric input by using directly connection would not only further enhance the existing security structure in the system of Cromer during startup of a device and access control but will also provide safeguards against attempt by unauthorized person to breach security of system during start-up or shut-down (Cromer: col.1 line 65 to col.2 line 5, and Teitelbaum: col.9 line 46 to line 65).

9.   Regarding Claim 48 Cromer teach and describe a propagated signal on which is instructions which is carried computer-executable instruction which when executed by a computing system performs a power gating, the method comprising.

a) asserting an activation signal responsive to a verification of a user biometric signature; and

b) gating, responsive to said activation signal, power from a power source to the electronic device operable from said power using a switch operably disposed between said power source and said electronic device wherein said electronic device is inoperable from said power source until said assertion of said biometric activation signal (Fig.1-3, col.2 line 34 to col.3 line 25, col.4 line 40 to col.5, line 5, and col.5 line 24 to col.6line 15).

Although the system disclosed by Cromer shows the features of the claimed limitation of controlling within a data processing system for the power supplied to the system .The system

of Cromer includes an internal power supply for receiving energy from an external source and supplying the energy to the system. The energy is full system power and is required for the system to be fully operable. The system is initially powered-off such that the energy is not initially supplied to the system. A power-on password is established. The internal power supply supplies the energy to the system only in response to a correct entry of the power-on password, wherein the system is inoperable prior to the correct entry of the power-on password.

However, Cromer does not specifically disclose gating functionality using biometric controlled switch.

In an analogous art, Teitelbaum, on the other hand discloses computing environment that relates to methods and device for receiving biometric input information and for providing biometric data to the a switch for establishing a communication link, such as start and stop of access control, between at least a user and the at least a device user is trying to access, and thus providing features and enabling services in dependence upon received biometric data (col.2 line 42 to line 52, and col.4 line 14 to col.15 line 10).

Therefore, It would have been obvious to one ordinary skilled in the art at the time of invention to combine the teachings of Cromer and Teitelbaum, because Teitelbaum's device and functionality combined with Cromer's power security unit (PSU), for controlling power to the system before the start-up, using biometric input by using directly connection would not only further enhance the existing security structure in the system of Cromer during startup of a device and access control but will also provide safeguards against attempt by unauthorized person to breach security of system during start-up or shut-down (Cromer: col.1 line 65 to col.2 line 5, and Teitelbaum: col.9 line 46 to line 65).

10.   Regarding Claim 49 Cromer teach and describe a biometric-apparatus for gating

power, comprising. means, responsive to a verification of a user biometric signature, for

asserting a biometric activation signal to enable a power source, and means, responsive to said

biometric activation signal, for gating power from said power source to an electronic device

operable from said power using a biometric-controlled switch operably disposed between said

power source and said electronic device wherein said electronic device is inoperable from said

power source until said assertion of said biometric activation signal (Fig.1-3, col.2 line 34 to

col.3 line 25, col.4 line 40 to col.5, line 5, and col.5 line 24 to col.6line 15).

Although the system disclosed by Cromer shows the features of the claimed limitation of

controlling within a data processing system for the power supplied to the system .The system

of Cromer includes an internal power supply for receiving energy from an external source and

supplying the energy to the system. The energy is full system power and is required for the

system to be fully operable. The system is initially powered-off such that the energy is not

initially supplied to the system. A power-on password is established. The internal power

supply supplies the energy to the system only in response to a correct entry of the power-on

password, wherein the system is inoperable prior to the correct entry of the power-on password.

However, Cromer does not specifically disclose gating functionality using biometric

controlled switch.

In an analogous art, Teitelbaum, on the other hand discloses computing environment that

relates to methods and device for receiving biometric input information and for providing

biometric data to the a switch for establishing a communication link, such as start and stop of

access control, between at least a user and the at least a device user is trying to access, and thus

providing features and enabling services in dependence upon received biometric data (col.2 line

42 to line 52, and col.4 line 14 to col.15 line 10).

Therefore, It would have been obvious to one ordinary skilled in the art at the time of

invention to combine the teachings of Cromer and Teitelbaum, because Teitelbaum's device

and functionality combined with Cromer's power security unit (PSU), for controlling power to

the system before the start-up, using biometric input by using directly connection would not

only further enhance the existing security structure in the system of Cromer during startup of a

device and access control but will also provide safeguards against attempt by unauthorized

person to breach security of system during start-up or shut-down (Cromer: col.1 line 65 to col.2

line 5, and Teitelbaum: col.9 line 46 to line 65).

11.   Claims 4-15, 18, 21, 25, 27-29, 32-37, 38, 41, and 44 are rejected applied as above

rejecting Claims 3, 24, and 26. Furthermore, the system of Cromer, and Teitelbaum teach and

describe a biometric access control of power gating provided to operate components of the

electronic device, wherein:

        - said biometric signature includes a fingerprint, a retinal pattern (Teitelbaum: col.1 line

45 to line 55),

        - a portable electronic device, a personal data assistant (PDA), includes a laptop computer

(Cromer: col.1 line 15 to line 32);

        - said power source includes a battery, a power supply, a direct power (Cromer: col.1 line

15 to line 32);

- said switch is integrated into said electronic, the power source, said biometric reader, and said switch is a state device for storing an operational mode (Teitelbaum:Fig.13-15, col.12 line 54 to line 58);

- said electronic device includes a plurality of BIOS routines and wherein said switch selectively activates one or more of said BIOS routines responsive to said activation signal (Teitelbaum: col.7 line 50 to col.9 line 15).

- said electronic device enables access to a set of resources responsive to an authentication and wherein said switch provides said authentication responsive to said activation signal (Cromer: Abstract, and Teitelbaum: col.2 line 28 to col.65).

- said gating step d) operation enablement includes initiating a boot sequence of said electronic device (Teitelbaum: col.7 line 50 to col.9 line 15).

12.   Claims 16,19, 22, 30-31, 39, 42, and 45 are rejected applied as above rejecting Claims 15, 18, 21, 29, 38, 41, and 44. Furthermore, the system of Cromer, and Teitelbaum teaches and describes a biometric access control of power gating provided to operate components of the electronic device, wherein:

- said operational mode maintains said gating of said power from said power source after receiving an asserted activation signal (Cromer: Fig.1-3, col1 line 58 to col.2 line 67).

- said biometric reader discriminates between a first user and a second user, with said activation signal identifying a particular one of said users (Teitelbaum: col.7 line 50 to col.9 line 15)

- biometric reader for asserting said activation signal responsive to said verification of

said biometric signature, the method further comprising discriminating between a first user and a

second user, with said activation signal identifying a particular one of said users (Teitelbaum:

col.7 line 50 to col.9 line 15)

13.   Claims 17, 20, 23, 40, 43, and 46 are rejected applied as above rejecting Claims 16, 19,

22, 39, 42, and 45. Furthermore, the system of Cromer, and Teitelbaum teaches and describes a

biometric access control of power gating provided to operate components of the electronic

device, wherein:

said operational mode is reset to disable said power from said power source when said

electronic device is inactivated pending reassertion of said activation signal (Cromer: Fig.1-3,

col1 line 58 to col.2 line 67).

said switch selectively activates said one or more said BIOS routine responsive to said

particular one user with said switch activating a different one or more of said BIOS routines for

said first user than activated for said second user (Teitelbaum: col.7 line 50 to col.9 line 15)

- said switch selectively enables access to one or more resources of said set of resources

responsive to said particular one user with said switch signaling enablement of a different one or

more resources for said first user than enabled for said second user (Teitelbaum: col.7 line 50 to

col.9 line 15);

- said portable electronic device includes a personal data assistant (PDA), and a laptop

computer (Cromer: col.1 line 15 to line 32);

resetting said operational mode to disable said power from said power source when said electronic device is inactivated pending a reassertion of said activation signal (Cromer: Fig.1-3, col1 line 58 to col.2 line 67).

- activating selectively said one or more said BIOS routine responsive to said particular one user wherein a different one or more of said BIOS routines are activated for said first user than are activated for said second user (Teitelbaum: col.7 line 50 to col.9 line 15)

- selectively enabling access to one or more resources of said set of resources responsive to said particular one user with a different one or more resources enabled for said first user than are enabled for said second user (Cromer: Fig.1-3, col.4 line 40 to col.5, line 5, and Teitelbaum: col.2 line 42 to line 52, and col.4 line 14 to col.15 line 10).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Syed Zia whose telephone number is 571-272-3798. The examiner can normally be reached on 9:00 to 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published applications

may be obtained from either Private PAIR or Public PAIR. Status information for unpublished

applications is available through Private PAIR only. For more information about the PAIR

system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR

system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would

like assistance from a USPTO Customer Service Representative or access to the automated

information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

sz
October 16, 2006